פורום שווי הוגן FVF (Fair Value Forum)

מפגש ינואר "ניהול סיכוני סייבר בסקטור הפיננסי והשירותי על רקע פרשת שירביט והאירועים האחרונים"

דברי פתיחה שלומי שוב

בוקר טוב לכולם,
בחרנו לעסוק הבוקר בנושא ניהול סיכוני הסייבר – זה לא נושא טריוויאלי לפורום שלנו שהוא פיננסי במהותו – אבל הגענו למסקנה שלמרות שמדובר בסיכון תפעולי – החשיבות שלו וההשלכות הפוטנציאליות רבות המימדים מגיעים לכדי כך שראוי שנדון בו. הטריגר לדיון הוא אמנם המקרים האחרונים לרבות שירביט – אבל חשוב להדגיש כי זהו לא נושא חדש. סיכוני הסייבר התפתחו בזירה העסקית באופן משמעותי מזה לפחות עשור עם המהפכה הדיגיטלית והם ילוו אותנו ביתר שאת ככל שהדיגיטציה תואץ וזה כנראה יקרה. אגב, בעקבות משבר הקורונה חווינו האצה מהירה של הדיגיטציה שניתן להניח שהגבירה את עוצמת הבעיה ואולי גם עוד לא הכל נחשף.

אין ספק שיחד עם שיפור ההגנות גם התוקפים משתכללים ככל שחולף הזמן ולכן זוהי מסוג החשיפות שלא תהיה להן כנראה אף פעם סגירה הרמטית ועל כן הדיון שלנו הוא במישור של ניהול הסיכון. אגב, הקושי המיוחד עם הנושא הזה הוא שלמנהלי הסיכונים באופן טבעי ולהבדיל אולי מסיכונים אחרים, יש פחות מומחיות מקצועית בתחום מאשר למשל במחלקות מערכות המידע ולכן יש קושי מובנה בניהול הסיכון הלא סטאטי הזה שתכופות משנה את פניו. כשמנהל סיכון נמצא בנקודת נחיתות מבחינת מומחיות לגבי סיכון מסויים זה תמיד יותר מאתגר.

אנחנו רגילים לייחס את הסיכון לגופים הפיננסיים – בין היתר לאור האירועים האחרונים, אך זה נובע מהעובדה שהדיגיטציה בגופים אלה שהם נותני שירותים במהותם מפותחת יחסית. אבל סיכון הסייבר הרבה יותר רחב והוא נוגע לכלל הגופים במשק – המשוואה מאד פשוטה: ככל שהדיגיטציה מתגברת - כל ענף כמובן בקצב שלו, הרי שגם הסיכון גדל. תסתכלו למשל כיום על רשתות קמעונאיות, קופות חולים ואפילו האוניברסיטאות שחטפו את ה"כאפה" של המשבר ועברו בבת אחת לדיגיטל – בקיצור בעיקר המגזר השירותי.

גם אם מסתכלים על האירועים האחרונים בסקטור הפיננסי יש כאן מצב מוזר שלכאורה לשלושת הרגולטורים הפיננסיים (ואולי גם נוסיף להם בהקשר של הסייבר גם את הרשות להגנת הפרטיות) יש את הסמכות ופחות את הידע והם מתרכזים בעיקר בדיווחים ודווקא למערך הסייבר הלאומי שיש את הידע והיכולת לעזור אין את הסמכות. גם עצם העובדה שכל רגולטור מוציא את ההוראות שלו בנפרד והן לא בהכרח אחידות היא מוזרה – הסתכלנו למשל לקראת הדיון על הגדרת אירוע סייבר בהוראות של המפקח על הבנקים ובהוראות רשות שוק ההון – שהם שני הרגולטורים הראשיים בתחום - ההגדרה לא זהה כך שיכול להיות מצב דברים שבו אירוע סייבר יוגדר כך למשל במערכת הבנקאית אבל לא בביטוח.

פורום שווי הוגן (Fair Value Forum) FVF

יש לשים לב שלרשות ני"ע – הרגולטור הפיננסי השלישי יש כאן שני כובעים – אחד כאחראית על הדיווחים של כלל החברות המדווחות והשני כמפקחת על קרנות הנאמנות ועל מנהלי התיקים (אגב, שיכולים להיות מאד קטנים ולכן לסבול מחסרון לגודל שיכול להיות מאד בעייתי בהקשר של הסייבר ולכן להציב אתגר לא פשוט).

עסקנו השנה בפורום בבעייתיות שנובעת מחוסר התאום והחפיפות בין שלושת הרגולטורים הפיננסיים בישראל – תחשבו למשל על בית השקעות שיש לו כמה רגולטורים – ובד"כ המחלקה שאחראית על הסייבר נמצאת למעלה אז היא צריכה לעמוד בכמה רגולציות. אגב, אני חושש מאותם מצבים שבהם לכאורה יש כפל רגולציה – לעיתים קורה בדיוק הפוך ונוצר וואקום כי כל רגולטור סומך על השני. מעבר לכך שיש כאן פוטנציאל לשונות במוכנות לסייבר בין גופים שונים בתוך הסקטור הפיננסי, המצב האידיאלי הוא שיהיה גוף אחד שלפי כללים אחידים יקבע את ההנחיות מצד אחד ויקבל את הדיווחים מהצד השני. מה שכן טוב יהיה אם ניקח את אירוע שירביט – שזה אירוע מתקפה על אמת כאירוע תירגול טוב לצורך תיאום רגולטורי – אני מבין שהיה תיאום בין כלל הרגולטורים במקרה זה וזה חשוב ואולי גם צריך לחשוב על שינוי מבני בנושא כהפקת לקחים.

נושא הדיווח למשקיעים על אירוע סייבר הוא לא טריוויאלי בכלל, במיוחד על רקע סף המהותיות שדורש הפעלת שיקול דעת והאינטרס הברור של המנהלים לא לדווח על מידע רגיש כזה. ההערכות הן ועשיתי לא מעט שיחות עם מומחים לקראת הדיון שהרוב המוחלט של האירועים לא מדווחים למשקיעים – ולפי מיטב הבנתי גם לא לרגולטורים הפיננסיים (אני לא מכליל כאן את הרשות להגנת פרטיות). וזה גם מעבר לשאלת ההגדרה של אירוע סייבר שגם היא אינה טריוויאלית. המקרים הספורים שאנחנו כן רואים הם בדרך כלל אלה שכבר הגיעו לתקשורת בדרך כזאת או אחרת – בד"כ על ידי לקוחות או צדדים שלישיים ופחות מיישום חובות דיווח. מה שמטריד אותי שאין עקביות בגילוי – יש כמה מקרים ספורדיים שעלו כמו בזמנו לאומי קארד וכעת שירביט. בדוח התקופתי השנתי אנחנו רואים בעיקר דיווח גנרי בסגנון המוכר של לצאת ידי חובה.

מבחינה חשבונאית, מבחן המהותיות הוא אחד ממבחני שיקול הדעת שהם תמיד יותר קשים כאשר יש כל כך הרבה רגישות ואינטרסים סביב המסקנה שלהם. הקביעה של מהותיות כאן צריכה להתבצע לפי גודל הפריצה ופוטנציאל הנזק שהפריצה מעידה עליו. חשוב לי כאיש חשבונאות להדגיש לכם - זה שחברה שילמה כופר בסכום לא מהותי לא מעיד על כך שזהו מידע לא מהותי. תחשבו לדוגמה על תשלום כופר של חצי מיליון שקל של תאגיד גדול – ככל הנראה לא מדובר בסכום מהותי – אבל אי אפשר להגיד שבהכרח זה לא מהותי לאור ההיבט האיכותי. הרי בעצם זה שהחברה היתה חשופה לפגיעה יכולות להיות משמעויות רבות קדימה. אגב, אני נותן את הדוגמה הזאת בד"כ לסטודנטים שלי בקורס תיאוריה חשבונאית כדי להמחיש להם מקרים מהותיים מבחינה איכותית אך לא כמותית. הבעיה היא שבמצב הדברים הנוכחי היכולת של רשות ניע לאכוף ולוודא שמידע שצריך להגיע למשקיעים אכן מגיע אליהם היא מאד מוגבלת, בלשון המעטה.

פורום שווי הוגן FVF (Fair Value Forum)

בשורה התחתונה יש כאן גם סתירה פנימית צורמת - הרי ככל שלא מדובר במידע מהותי למשקיעים אז מדוע אנחנו עוסקים בנושא הזה היום ומדוע כל כך הרבה אנשים רציניים התאספו לדיון הזה? כפי שציינו בחומר הרקע המחקרים מעידים על השפעה לא מהותית על מחיר המניה של דיווח על אירועי סייבר – אבל כנראה שמה עומד מאחורי זה הוא שדווקא האירועים הלא מהותיים הם אלה שמדווחים. פרופ' אלי אמיר, ד"ר שי לוי וצפריר ליבנה מאונ' תל אביב הראו את זה במחקר שלהם דרך הממצא לפיו דווקא כאשר הגילוי נובע מהדלפה ולא מיוזמת החברה ההשלכות שלו על מחיר המניה משמעותיות. המקרה של הסייבר הוא דוגמה חדה שממחישה לדעתי בעיה רחבה יותר בדיווחי חברות בשוק ההון. חברות אוהבות לדווח ארוכות על מה שפחות חשוב ולגבי הדברים החשובים באמת מנסים בדרך כזאת או אחרת לצאת ידי חובה דרך ניסוחים גנריים. דוגמה שממחישה זאת היטב היא המקרה המוכר של יאהו שב- 2016 באיחור של שנתיים-שלוש נאלצה להודות, בעקבות זה שכ- 200 מיליון שמות חשבון, מיילים וסיסמאות הוצעו למכירה בדארק-נט, וזה קרה ערב הקלוזינג של עסקת הרכישה שלה - מה שהוביל להתאמת המחיר מטה בכ- 8%.

בכל הנושא הזה של מרחב הסייבר יש לא מעט היבטי מאקרו לרבות למשל בהקשר של התחרות במגזר הפיננסי וכניסת חברות פינטק חדשות. עולות כאן גם שאלות ברמה הלאומית שהרי יש כאן גם ענייני טרור ועולה שאלה מה תפקיד המדינה בהגנה על המגזר העסקי – כי אם במקרה של שירביט זאת התקפת טרור מה ההבדל בין זה לבין הגנה של המדינה עלינו מהתקפות טילים למשל? כלומר, ראוי לשאול היום בדיון מדוע המדינה והרגולטורים לא עוברים למודל של הגנה מצרפית? מצד שני צריך גם להגיד שעולות כאן גם שאלות בנגע להגבלים עסקיים ולא פחות מכך שאלות כבדות משקל בנוגע ליכולת של המדינה להתערב בעסקים, כפי שעלה בזמנו בעקבות פרסום המזכר של חוק הסייבר ב- 2018 – אגב חקיקה שלא התקדמה מאז.

צריך להבחין בין דיווח למשקיעים לבין דיווח לרגולטור או לא פחות חשוב ואף אולי יותר הוא שיתוף המידע בין הגופים הפיננסים לבין עצמם ובין הגופים לבין הספקים שלהם. ממש לאחרונה ראינו את המקרה של עמיטל שהיא חברת תוכנה המשווקת תוכנות לחברות העוסקות בעמילות מכס שהתמודדה עם מתקפת סייבר ובעקבות כאן נפגעו גם הלקוחות שלה – חברות עמילות מכס כמו אוריין חברה ציבורית שדיווחה גם היא על מתקפה.
כפורום שנקרא שווי הוגן חשוב לנו היום גם לנסות לתרגם את הסיכון התפעולי לערכים כספיים ולכן תהליך החיתום הביטוחי מאד מעניין אותנו. בגדול, הפוליסות נועדות לבטח הן את החברה הנתקפת והן את הלקוחות הנפגעים אבל נשאלת השאלה, כיצד ביטוחי הסייבר מתומחרים? כמובן שבתמחור הביטוח נלקחים בחשבון גורמים רבים הן במישור של מידת החשיפה והן במישור המוכנות של החברה, אבל הכימות הזה לא טריוויאלי בין היתר לאור העובדה שהתחום כל הזמן מתפתח וקשה להסיק לאור נתוני העבר כמו שקורה בד"כ בתחומים אחרים. אנחנו נעסוק בדיון גם בכך ובמתודולוגיות אפשריות. בכל מקרה, ממה שאני מבין הפוליסות משפות לגבי הוצאות יעוץ בעת משבר להגנה על המוניטין ועל אובדן ההכנסות לתקופת השיפוי אבל אינן מכסות נזק פוטנציאלי לשווי המוניטין של החברה הנפגעת - וזאת נקודה חשובה שגם נרצה לדבר עליה היום. שאלת הנזק למוניטין היא לא טריוויאלית.

פורום שווי הוגן FVF (Fair Value Forum)

הסתכלתי קצת לקראת הדיון על הדוחות השנתיים של הסקטור הפיננסי ל- 2019 וראיתי שחמשת הבנקים, למעט דיסקונט מגדירים את רמת החומרה של סיכון הסייבר כבינונית ולא כגבוהה. אגב, גם ישראכרט מגדירה זאת כבינונית. מנגד, חלק מחברות ביטוח מגדירות אותו כגבוה. כך למשל, מגדל מסווגת את סיכון הסייבר כהשפעה גבוהה בעוד כלל ביטוח כהשפעה בינונית. מעניין להשוות בין הביטוח לבנקים עד כמה זה נובע מפערים ברמת המוכנות שהרי התפיסה היא שהבנקים מוכנים יותר אבל יתכן שזה נובע גם מפוטנציאל הנזק ביחס לעוצמת ההון. בבנקים עשו לפני כשנה תרחיש קיצון לאירוע סייבר וממה שאני מבין לא התגלתה השפעה משמעותית על הרווח – עוד מעט נשמע מדני חחיאשווילי סגן המפקח שנמצא איתנו על כך. יהיה מעניין לראות את ההתפתחויות בנושא בקרוב והאם נראה עליה במדרגות הסיכון של הסייבר בדוחות הקרובים.

אין ספק שהמודעות בגופים הפיננסיים לסיכון הסייבר היא גבוהה יותר וכפועל יוצא גם רמת המוגנות שלהם גבוהה יותר, אבל זה כאמור משליך גם על יתר החברות במשק. אגב, שימו לב שחברות הביטוח יכול להיפגע גם בעוד מישור – המחויבות שנגזרת מפוליסות ביטוח שהן מנפיקות דווקא לא בתחום הסייבר – לא בהכרח שניתן יהיה להחריג את הסייבר מנזקים אחרים שנגרמו – אפילו תקיפות שתוצאתן נזקים פיזיים – ואנחנו היינו עדים לאחרונה לכל מיני התפתחויות בנושא.

זה מתחבר לנושא של אחריות דירקטורים ומנהלים – אין ספק שהתהליך הביטוחי מסייע מאד להגנה, אבל הוא כמובן לא ממצה את הסיכון והאחריות, אבל מהווה נקודת מוצא טובה. התפקיד של הדירקטוריון הוא קודם כל ניהול הסיכון וצמצומו אבל גם כמובן במקרה של תקיפה – כפי שראינו באירועים האחרונים. נמצאים פה נציגים הבכירים בנושא של הרגולטורים הפיננסיים ומנהלי הסיכונים בכל הגופים הפיננסיים המובילים בישראל. זה ברור שלגבי גופים חיוניים/קריטיים גם בסקטור הפיננסי כמו הבורסה לניע המדינה מעורבת אבל אנחנו רוצים דווקא לדבר היום על כלל החברות שאינן גופים קריטיים או ציבוריים - לרבות מהמגזר הפיננסי.

אנחנו נשמע עוד מעט את הרגולטורים השונים. ממה שאני מבין מערך הסייבר אוסף נתונים על האירועים השונים ונשמח לשמוע בהמשך ממיטל אריק ממערך הסייבר על המגמה של האירועים בראיית מאקרו - שאני מניח שנמצאת במגמת עליה בשנים האחרונות. בכל מקרה אני חושב שראוי להסדיר את נושא הסייבר ברמה משקית.